

Clear Discarded Storage that Contained Secrets and Do Not Read Uninitialized Storage

William L. Fithen, Software Engineering Institute [vita³]

Copyright © 2005 Carnegie Mellon University

2005-10-03

Failing to initialize storage can introduce vulnerability.

Description

When allocated, storage may not have been initialized, meaning that whatever was left in storage from its previous use is still there. If that storage might contain leftover secrets, like passwords, then accidentally disclosing that data amounts to a security leak—of information from the previous user.

When your system, in turn, deallocates storage that contains secrets, it may be leaking those secrets to the *next* user of the storage.

References

- | | |
|---------------|--|
| [Thompson 05] | Thompson, Herbert & Chase, Scott. <i>The Software Vulnerability Guide</i> . Charles River Media, 211-222. 2005. |
| [VU#412115] | Lanza, Jeffrey P. <i>Network device drivers reuse old frame buffer data to pad packets</i> . 2003. http://www.kb.cert.org/vuls/id/412115 . |

SEI Copyright

Carnegie Mellon University SEI-authored documents are sponsored by the U.S. Department of Defense under Contract FA8721-05-C-0003. Carnegie Mellon University retains copyrights in all material produced under this contract. The U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce these documents, or allow others to do so, for U.S. Government purposes only pursuant to the copyright license under the contract clause at 252.227-7013.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For inquiries regarding reproducing this document or preparing derivative works of this document for external and commercial use, including information about “Fair Use,” see the [Permissions](#)¹ page on the SEI web site. If you do not find the copyright information you need on this web site, please consult your legal counsel for advice.

3. daisy:320 (Fithen, William L.)

1. <http://www.sei.cmu.edu/about/legal-permissions.html>

Velden

Naam	Waarde
Copyright Holder	SEI

Velden

Naam	Waarde
is-content-area-overview	false
Content Areas	Knowledge/Guidelines
SDLC Relevance	Implementation
Workflow State	Publishable